Cassandra Crossing/ Log4j—stavolta ci è andata bene

(491)—Il baco del secolo poteva essere utilizzato in maniera distruttiva, e non è accaduto; adesso cosa succede?

Cassandra Crossing/ Log4j—stavolta ci è andata bene
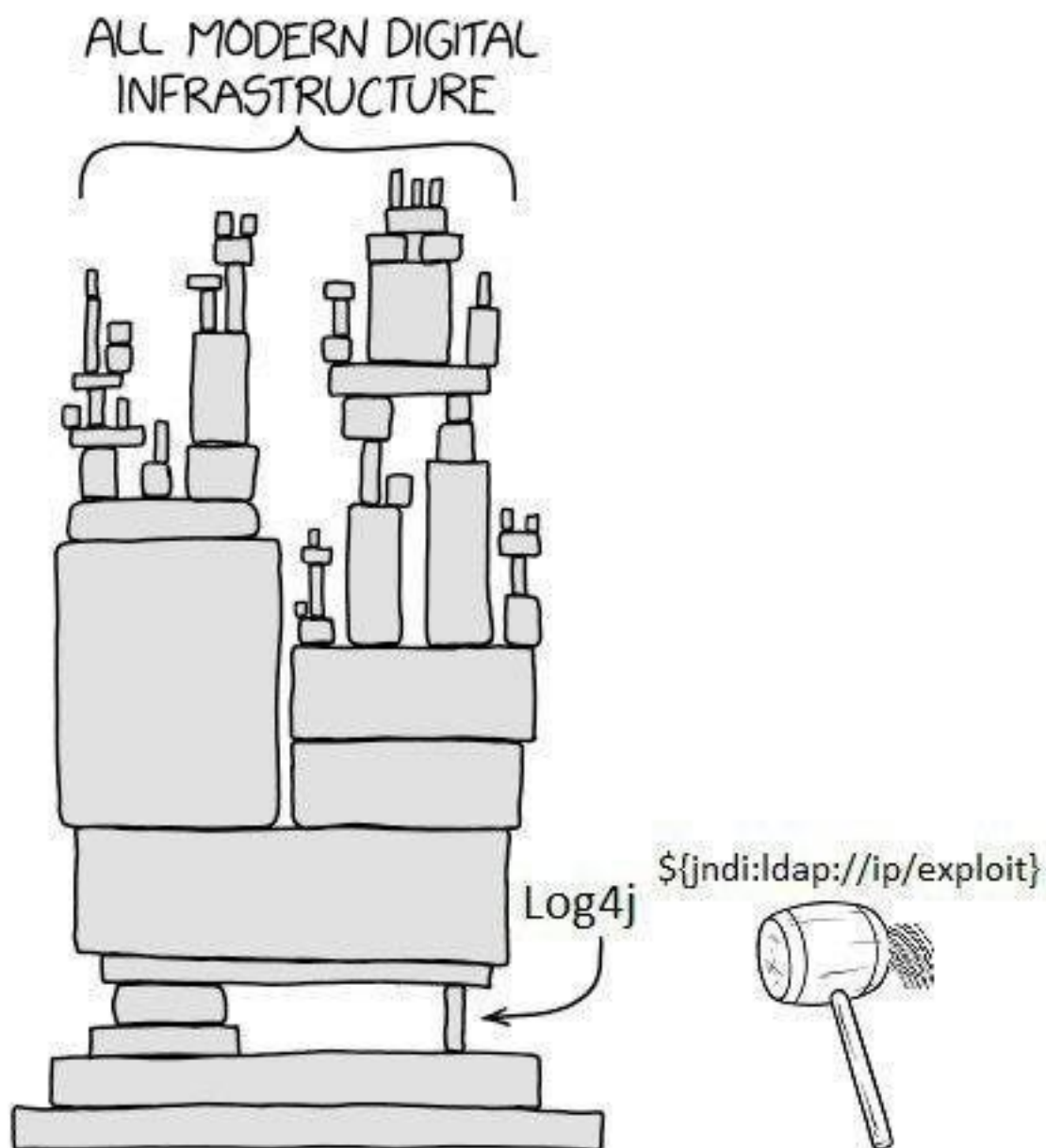
Figure 1:

(491)—Il baco del secolo poteva essere utilizzato in maniera distruttiva, e non è accaduto; adesso cosa succede?

16 dicembre 2021—Come i 24 infettabili lettori di Cassandra sanno, l'argomento della prossima catastrofe sulla Rete è sempre stato in primo piano su queste pagine, particolarmente quando

legato alla complessità del software.

L'attuale tema "caldo" è certamente il baco della libreria log4j; come spesso accade per gli argomenti molto dibattuti, questo impedisce di mettere in prospettiva le questioni principali, soffocate dall'analisi dei dettagli, quando non addirittura dalle chiacchiere da salotto.

L'aspetto trascurato e riassuntivo dell'"*affaire*" Log4j è presto detto; "**Questa volta ci è andata davvero bene**".

I sistemisti dell'intero orbe terraqueo, inclusi quelli della NASA, di SpaceX e delle varie agenzie spaziali nazionali, che stanno lavorando da giorni in condizione di totale emergenza, potrebbero non essere d'accordo; forse per lo stress potrebbero anche reagire molto male ad una simile affermazione.

Cerchiamo quindi non solo di esporla, ma di motivarla, e per far ciò, come al solito, dobbiamo inquadrare la cosa da un punto di vista storico e riavvolgere il nastro; questa volta ad una data tanto precisa quanto lontana, e cioè il **25 gennaio 2003**.
Quel giorno si verificò il secondo più grave incidente globale della Rete (secondo solo al Morris Worm del 2 novembre 1988, che causò due giorni di distruzione della neonata Internet)

Quel sabato SQLSlammer, un worm standalone in grado di autoreplicarsi in tempi brevissimi, anche perché operante esclusivamente in RAM, infettò 75000 server in meno di 10 minuti, e causò il più vistoso e prolungato rallentamento planetario di Internet.

Il rallentamento non fu causato da azioni malevole del worm, che come il Morris Worm non era malevolo perché non faceva niente ma si limitava ad autoreplicarsi, ma solo dal picco di traffico generato dai server colpiti, traffico che mandò in crisi, ed in alcuni casi fece anche collassare, i router principali di Internet.

SQLSlammer tra l'altro sfruttava una falla ben nota di Microsoft SQL server, che era a conoscenza di Microsoft dal 24 luglio 2002, la quale aveva rilasciato abbastanza prontamente una ben poco considerata e propagandata patch software, disponibile quindi ben sei mesi prima dell'evento, e che all'epoca ben pochi amministratori di sistema avevano considerato ed installato.

Nel caso di SQLSlammer il fatto che la soluzione fosse immediatamente disponibile ebbe l'effetto positivo di permettere un relativamente veloce ritorno alla normalità; installare la patch e fare un reboot, che rimuoveva SQLSlammer dalla RAM, era sufficiente.

Forse, inquadrandolo in prospettiva, questo fatto apparentemente positivo è stato invece addirittura negativo, perché ha portato ad una sottovalutazione dell'accaduto, anzi ad un suo rapido oblio.

Oggi, venti anni di sviluppo del malware hanno prodotto software capaci di sfruttare i bug in maniera modulare, efficiente, flessibile e, quando necessario, in modo completamente automatico; un esempio per tutti la botnet Mirai.

Ora supponiamo che il bug di Log4j, che ricordiamo:

- è cross platform;
- colpisce potenzialmente qualunque piattaforma e qualunque sistema operativo che usi Apache e/o Java;
- non aveva nessuna patch disponibile:
- permette l'iniezione e l'esecuzione via Internet di software arbitrario sulla macchina colpita

fosse stato sfruttato da una Botnet strategicamente programmata da uno degli attori della scena Malware/Cyberwarware.

Sarebbe stato tranquillamente possibile trovarsi di fronte al crash, o peggio ancora alla compromissione e presa di controllo totale della maggior parte dei server esposti su Internet, fatto che avrebbe richiesto la sconnessione, la reinstallazione completa, e l'applicazione di patch per ogni singolo server. Ripeto per chi non avesse percepito l'immane lavoro necessario rispetto agli altri casi, reinstallare e patchare ogni-singolo-server-esposto-su-internet, fisico, virtuale o dockerizzato che fosse.

Un incubo al cui confronto il recovery da SQLServer od anche dal Morris Worm sembrano dei semplici inconvenienti passeggeri.

Cassandra ama farla breve, e non è necessario ripetere i concetti, inanellando buzzword e superlativi per allungare la narrazione.

Alla fin della fiera ed buona sostanza, **dove è il problema oggi**?

Domandiamoci quanto hanno imparato negli ultimi venti anni i "*decisori di Internet*"; i sistemisti, i loro manager che devono chiedere budget per la sicurezza informatica ed il disaster recovery ed i loro consigli di amministrazione che dovrebbero decidere di **investire montagne di quattrini per mitigare il prossimo "Cigno Nero" di Internet, come quello che Log4j avrebbe potuto causare.**

Le cause della sistematica sottovalutazione della sicurezza informatica da parte delle aziende sono ancora tutte li; troppo spesso la reazione agli incidenti è un maggiore investimento in polizze assicurative ed in public relation, piuttosto che per la sicurezza informatica ed operativa.

E non dimentichiamo che una nuova classe di attori "nazionali" e di organizzazioni criminali sta ammassando armi informatiche negli arsenali, piccoli e grandi, pronti ad essere usati come arma in guerre tradizionali od in attentati terroristici.

Se fiumi di soldi non verranno spesi **realmente** in miglioramenti della sicurezza informatica ed operativa da tecnici e sistemisti, e non dirottati da funzionari e manager verso altri obbiettivi, vorrà dire che nulla sarà cambiato, e che la prossima botnet, il prossimo attacco da parte di una attore malevolo od il primo atto della prima guerra cibernetica potranno consistere nella disabilitazione prolungata di Internet e delle sue risorse, operata anche, ove occorresse, in maniera selettiva.

Sconnessi, al buio ed all'asciutto.

Lo scenario tratteggiato in queste poche righe dalla vostra profetessa preferita è abbastanza spaventoso?

Vi ha terrorizzato, od almeno preoccupato seriamente?

Speriamo; **in questo caso Cassandra sarà riuscita a fare il proprio mestiere**.

By Marco A. L. Calamari on December 17, 2021.

Canonical link

Exported from Medium on August 27, 2025.